Docket No.: 67161-089 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Shigenori MIYAUCHI, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: August 26, 2003	:	Examiner: Unknown

For: ENCRYPTION CIRCUIT ACHIEVING HIGHER OPERATION SPEED

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claims the priority of:

Japanese Patent Application No. 2002-310009, filed October 24, 2002

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:tlb
Facsimile: (202) 756-8087
Date: August 26, 2003

日　本　国　特　許　庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１０月２４日

出願番号
Application Number: 特願２００２－３１０００９

[ST.10/C]: [ＪＰ２００２－３１０００９]

出願人
Applicant(s): 三菱電機株式会社

２００２年１１月２６日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００２－３０９３４８３

【書類名】　特許願

【整理番号】　541973JP01

【提出日】　平成14年10月24日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

H04L　9/14

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　宮内　成典

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　山口　敦男

【特許出願人】

【識別番号】　000006013

【氏名又は名称】　三菱電機株式会社

【代理人】

【識別番号】　100064746

【弁理士】

【氏名又は名称】　深見　久郎

【選任した代理人】

【識別番号】　100085132

【弁理士】

【氏名又は名称】　森田　俊雄

【選任した代理人】

【識別番号】　100083703

【弁理士】

【氏名又は名称】　仲村　義平

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【選任した代理人】

【識別番号】　100098316

【弁理士】

【氏名又は名称】　野田　久登

【選任した代理人】

【識別番号】　100109162

【弁理士】

【氏名又は名称】　酒井　將行

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号回路

【特許請求の範囲】

【請求項１】　接続された複数の演算回路と、

前記複数の演算回路を制御して、暗号化または復号の制御を行なう制御回路とを含んだ暗号回路であって、

前記複数の演算回路はそれぞれ、演算データを保持する第１のレジスタと、

前記第１のレジスタに保持される演算データに対して加減算を実行する加減算回路と、

前記加減算回路による演算結果に対して右シフトを実行する右シフト回路と、

前記右シフト回路による演算結果を保持する第２のレジスタとを含み、

第１の演算回路の加減算回路は、第２の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を第３の演算回路へ出力し、

前記第１の演算回路の右シフト回路は、前記第３の演算回路からのシフトイン信号を用いて右シフトを実行し、右シフトによって発生するシフトアウト信号を前記第２の演算回路へ出力する、暗号回路。

【請求項２】　前記制御回路は、演算データを分割して前記複数の演算回路の第１のレジスタに格納する、請求項１記載の暗号回路。

【請求項３】　前記第１の演算回路の加減算回路は、第１のクロックで演算データを確定し、

前記第３の演算回路の加減算回路は、前記第１のクロックよりも１クロック遅れた第２のクロックで演算データおよび前記第１の演算回路からのキャリーアウトを確定する、請求項１または２記載の暗号回路。

【請求項４】　前記第１の演算回路の加減算回路は、第１のクロックで演算データを確定し、

前記第１の演算回路の第２のレジスタは、前記第１のクロックよりも１クロック遅れた第２のクロックで最上位ビット以外のビットが書込まれ、前記第２のクロックよりも半クロック遅れた第３のクロックで最上位ビットが書込まれる、請

求項１または２記載の暗号回路。

【請求項５】　前記複数の演算回路は、キャリーアウト信号およびシフトアウト信号がループするように接続される、請求項１～４のいずれかに記載の暗号回路。

【請求項６】　前記複数の演算回路のそれぞれは、さらに前記第２のレジスタに保持される演算結果に対して左シフトを実行する左シフト回路を含み、

前記第１の演算回路の左シフト回路は、前記第２の演算回路からのシフトイン信号を用いて左シフトを実行し、左シフトによって発生するシフトアウト信号を前記第３の演算回路へ出力する、請求項１～５のいずれかに記載の暗号回路。

【請求項７】　前記第１の演算回路はさらに、前記第３の演算回路からのシフトイン信号と、前記第１の演算回路の左シフト回路からのシフトイン信号とを選択的に前記第１の演算回路の加減算回路へ出力するセレクタを含む、請求項６記載の暗号回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、使用される情報の暗号化技術および復号技術に関し、特に、べき乗剰余演算、モンゴメリ演算、加減算などの演算によってデータを暗号化および復号する暗号回路に関する。

【０００２】

【従来の技術】

情報通信技術の発展に伴い、情報ネットワーク上のセキュリティの確保（データの盗用や破壊を防止すること）が重要視されるようになってきている。そのため、情報の暗号化技術および復号技術が採用されることが多く、その適用分野は単なる情報通信分野に留まらず、交通、金融、医療、流通等の身近な分野にまで広がりつつある。この種の暗号化技術および復号技術には、高度なセキュリティを単純な原理によって実現できることが要求される。

【０００３】

これに関連する技術として、特開平５－３２４２７７号公報および特開２００

２－２２９４４５号公報に開示された技術がある。

【０００４】

特開平５－３２４２７７号公報に開示された暗号通信方法は、剰余演算Ｑ＝Ａ・ＢmodＮおよびべき乗剰余演算Ｃ＝M^{e}modＮを、Ｎと素な整数Ｒを用いた同形の演算Ｚ＝Ｕ・Ｖ・R^{-1}modＮの繰返しにより実現するものである。

【０００５】

また、特開２００２－２２９４４５号公報に開示されたべき乗剰余演算回路は、鍵ｅを保持するｅレジスタ、モンゴメリ変換をする乗算Ｙを保持するＹレジスタ、鍵Ｎを保持するＮレジスタ、モンゴメリ変換の演算時に行なう２Ｂ＋Ｎの値を保持するＢ２Ｎレジスタ、平文Ｘを保持するＸレジスタ、暗号化および復号のための演算を行なう演算回路、演算結果Ｐを保持するＰレジスタなどを含み、高速処理を可能としたものである。

【０００６】

【特許文献１】

特開平５－３２４２７７号公報

【０００７】

【特許文献２】

特開２００２－２２９４４５号公報

【０００８】

【発明が解決しようとする課題】

現代の暗号は、秘密鍵を計算によって見つけることが時間的に困難であることを安全性の根拠としているものが多い。たとえば、ＲＳＡ（Rivest-Shamir-Adleman scheme）暗号を用いる場合、２つの素数の積である整数Ｎ（Ｎ＝ｐ×ｑ、ｐおよびｑは素数）を短時間で素因数分解することの難しさが安全性の根拠となっている。このことは、裏を返せば、今後コンピュータ等の計算機の性能が向上するに伴い、ＲＳＡ暗号の安全性を確保するためには、選択する素数ｐおよびｑの桁数を増やさなければならないことを意味している。

【０００９】

ここで、上述した特開平５－３２４２７７号公報および特開２００２－２２９

４４５号公報に開示された発明によって、ビット長の長い暗号回路を構成した場合を考える。最も簡単な方法は、レジスタ群を増やして暗号回路を変更することである。しかし、レジスタ群が増加した分だけ演算時間が増加するとともに、レジスタの増加分だけ暗号回路が大きくなるため得策ではない。

【００１０】

また、加減算回路が一度に扱えるビット長を、たとえば１２８ビットから２５６ビットに拡張した場合、加減算時におけるキャリーの伝播経路が長くなるため、動作周波数を上げることが困難になるといった問題点がある。

【００１１】

本発明は、上記問題点を解決するためになされたものであり、その目的は、暗号回路の動作クロック周波数を高くでき、演算速度の高速化を図ることが可能な暗号回路を提供することである。

【００１２】

【課題を解決するための手段】

請求項１に記載の暗号回路は、接続された複数の演算回路と、複数の演算回路を制御して、暗号化または復号の制御を行なう制御回路とを含む。また、複数の演算回路はそれぞれ、演算データを保持する第１のレジスタと、第１のレジスタに保持される演算データに対して加減算を実行する加減算回路と、加減算回路による演算結果に対して右シフトを実行する右シフト回路と、右シフト回路による演算結果を保持する第２のレジスタとを含む。第１の演算回路の加減算回路は、第２の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を第３の演算回路へ出力し、第１の演算回路の右シフト回路は、第３の演算回路からのシフトイン信号を用いて右シフトを実行し、右シフトによって発生するシフトアウト信号を第２の演算回路へ出力する。

【００１３】

【発明の実施の形態】

まず、本出願人が出願した特開２００２－２２９４４５号公報、特願２００１－１６３７１９号および特願２００２－２８６１８２号に開示した暗号回路について簡単に説明する。

【００１４】

図１は、本出願人が出願した暗号回路の概略構成を示すブロック図である。この暗号回路１０は、演算回路１２と、演算回路１２を制御して、べき乗剰余演算、モンゴメリ演算、加減算などの演算を実行する制御回路１１とを含む。

【００１５】

図２は、演算回路１２の概略構成を示すブロック図である。演算回路１２は、鍵ｅを保持する４本のｅレジスタ１２１と、モンゴメリ変換をする乗数Ｙを保持する４本のＹレジスタ１２２と、平文Ｘを保持する４本のＸレジスタ１２３と、鍵Ｎを保持する４本のＮレジスタ１２４と、モンゴメリ変換の演算時に行なう２Ｂ＋Ｎの値を保持する４本のＢ２Ｎレジスタ１２５と、１２８ビットの加減算回路１２６と、加減算回路１２６から出力される演算結果の最上位ビットの桁上り（キャリー）を保持する保持回路１２７と、１２８ビットの右シフト回路１２８と、右シフト回路１２８によって右シフト処理が行なわれる際に発生する最下位ビットの桁落ち（シフトアウト）を他の右シフト処理時にシフトイン信号として使用するために保持する保持回路１２９と、右シフト回路１２８から出力される演算結果を一時的に保持する複数のＰレジスタ１３０と、１２８ビットの左シフト回路１３１と、左シフト回路１３１によって左シフト処理が行なわれる際に発生する最上位ビットの桁上り（シフトアウト）を他の左シフト処理時にシフトイン信号として使用するために保持する保持回路１３２とを含む。

【００１６】

べき乗剰余演算、モンゴメリ演算、ＲＳＡ暗号などの演算処理は、主として加算、減算、乗算および除算の繰返しによって実現されるため、制御回路１１が図２に示す演算回路１２を制御してそれぞれの演算アルゴリズムにしたがって演算を繰返し行なわせることによってこれらの演算処理が可能になる。なお、演算アルゴリズムの詳細は上述した文献を参照されたい。

【００１７】

（第１の実施の形態）

図３は、本発明の第１の実施の形態における暗号回路の概略構成を示すブロック図である。この暗号回路２０は、暗号回路２０の全体的な制御を行なう制御回

路２１と、４つの演算回路０～３（２２～２５）とを含む。本実施の形態においては、暗号方式としてＲＳＡ暗号を想定し、演算長として５１２ビットを想定してるが、これに限定されるものではない。

【００１８】

制御回路２１は、外部から受けた演算に必要となるデータをデータバスを介して演算回路０～３（２２～２５）へ出力し、データバスを介して演算回路０～３（２２～２５）から受けた演算結果を外部へ出力する。また、制御回路２１は、ＲＳＡ暗号化または復号のアルゴリズムにしたがって演算回路０～３（２２～２５）へ制御信号を出力し、演算処理を制御する。

【００１９】

図４は、演算回路０～３（２２～２５）の内部構成を説明するためのブロック図である。演算回路０～３（２２～２５）のそれぞれは、鍵ｅを保持するｅレジスタ３１と、暗号化された平文Ｙを保持するＹレジスタ３２と、暗号化の対象となる平文Ｘを保持するＸレジスタ３３と、鍵Ｎを保持するＮレジスタ３４と、１２８ビットの加減算回路３５と、1.２８ビットの右シフト回路３６と、右シフト回路３６から出力される演算結果を一時的に保持するＰレジスタ３７と、１２８ビットの左シフト回路３８とを含む。

【００２０】

加減算回路３５は、ｅレジスタ３１、Ｙレジスタ３２、Ｘレジスタ３３またはＮレジスタ３４に保持されるデータに対して加算または減算を行ない、演算結果を右シフト回路３６へ出力する。また、加減算回路３５は、演算結果の最上位ビットの桁上り（キャリー）を他の演算回路へキャリーアウト信号として出力し、他の演算回路からのキャリーアウト信号をキャリーイン信号として入力し、最下位ビットに設定する。

【００２１】

右シフト回路３６は、加減算回路３５から出力された加減算結果を右シフトし、そのときに発生する最下位ビットの桁落ち（シフトアウト）を右シフトアウト信号として他の演算回路へ出力する。また、右シフト回路３６は、他の演算回路からのシフトアウト信号をシフトイン信号として入力し、最上位ビットに設定す

る。

【００２２】

左シフト回路３８は、Ｐレジスタ３７に保持される値を左シフトし、そのときに発生する最上位ビットの桁上り（シフトアウト）を左シフトアウト信号として他の演算回路へ出力する。また、左シフト回路３８は、他の演算回路からのシフトアウト信号をシフトイン信号として入力し、最下位ビットに設定する。

【００２３】

制御回路２１は、５１２ビットの演算データを１２８ビットずつに分割し、演算回路０～３（２２～２５）のぞれぞれのｅレジスタ３１、Ｙレジスタ３２、Ｘレジスタ３３またはＮレジスタ３４に格納する。たとえば、ｅレジスタに５１２ビットの演算データを格納する場合、演算回路０（２２）内のｅレジスタ３１に演算データのビット０～１２７を格納し、演算回路１（２３）内のｅレジスタ３１に演算データのビット１２８～２５５を格納し、演算回路２（２４）内のｅレジスタ３１に演算データのビット２５６～３８３を格納し、演算回路３（２５）内のｅレジスタ３１に演算データのビット３８４～５１１を格納する。

【００２４】

演算回路０～３（２２～２５）におけるデータ演算は１クロック単位で実施され、演算回路０（２２）から上位方向（演算回路０→１→２→３）にキャリーが伝播される。右シフト回路３６による右シフト処理はクロックによって遅らされることなく、上位の演算回路の動作クロックを利用して下位の演算回路にシフトインが行なわれる。この機能を実現するために、制御回路２１は、Ｐレジスタ３７へのビット０～１２６のライト信号と、ビット１２７のライト信号とを独立制御している。

【００２５】

図５は、演算回路における演算データの入力タイミングおよびＰレジスタ３７へのデータ書込みタイミングを説明するためのタイミングチャートである。クロックＴ１の立下りで演算回路０（２２）への入力データが確定すると、加減算回路３５からキャリーアウト信号が出力される。

【００２６】

また、クロックＴ２の立下りで演算回路０（２２）内のＰレジスタ３７にデータのビット０～１２６が書込まれると共に、上位の演算回路１（２３）への入力データが確定する。このタイミングでは、上位の演算回路１（２３）の右シフトアウト信号が確定していないので、演算回路０（２２）内のＰレジスタ３７にデータのビット１２７を書込むことができない。したがって、クロックＴ３の立上りで演算回路０（２２）内のＰレジスタ３７にデータのビット１２７が書込まれる。なお、他の下位の演算回路と上位の演算回路との間の信号のタイミングは、この演算回路０（２２）と演算回路１（２３）との間の信号のタイミングと同様である。

【００２７】

図６は、演算回路における演算データの入力およびＰレジスタ３７へのデータ書込みが連続的に行なわれる場合のタイミングを説明するためのタイミングチャートである。図５に示すタイミングチャートとほぼ同様であるが、各クロックサイクルで１２８ビットの演算データが処理されることを示している。すなわち、演算回路０～３（２２～２５）は、５１２ビットの演算データの処理を行なうのに４クロック必要である。しかし、乗算やモンゴメリ乗算剰余演算の繰返し演算など、加減算の結果の正負が次の演算種別に反映されない場合には、演算の完了を待たずに次の加減算を行なうことができるので、パイプライン的に処理を行なうことができ、実効的にはその１／４のクロック数（１クロック）で演算を行なうことができる。

【００２８】

以上説明したように、本実施の形態における暗号回路によれば、演算データを複数に分割し、複数の演算回路にそれぞれの演算データを演算させ、キャリーアウトおよびシフトアウトのみを上位の演算回路または下位の演算回路に出力するようにしたので、演算回路の回路規模を縮小することができると共に、キャリーの伝播経路を短くでき、動作クロック周波数を高くすることが可能となった。

【００２９】

また、１２８ビットの演算データを処理する演算回路と比較すると、同じクロック数で４倍の演算データを処理することができ、演算速度の高速化を図ること

が可能となった。

【００３０】

（第２の実施の形態）

図７は、本発明の第２の実施の形態における暗号回路の概略構成を示すブロック図である。本実施の形態における暗号回路は、図３に示す第１の実施の形態における暗号回路と比較して、演算回路３から出力されるキャリーアウト信号および左シフトアウト信号が演算回路０に入力され、演算回路０から出力される右シフトアウト信号が演算回路３に入力され、演算回路間をキャリーアウト信号およびシフトアウト信号がループしている点が異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。なお、本実施の形態においては、暗号方式としてＲＳＡ暗号を想定し、演算長として１０２４ビットを想定してるが、これに限定されるものではない。

【００３１】

図８は、本発明の第２の実施の形態における演算回路０～３（４１～４４）の内部構成を説明するためのブロック図である。本実施の形態における演算回路０～３（４１～４４）は、図４に示す第１の実施の形態における演算回路０～３（２２～２５）と比較して、ｅレジスタ、Ｙレジスタ、Ｘレジスタ、ＮレジスタおよびＰレジスタが２本ずつ設けられている点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００３２】

制御回路２１は、１０２４ビットの演算データを１２８ビットずつに分割し、演算回路０～３（４１～４４）のぞれぞれのｅ０レジスタ５１、Ｙ０レジスタ５２、Ｘ０レジスタ５３、Ｎ０レジスタ５４、ｅ１レジスタ６１、Ｙ１レジスタ６２、Ｘ１レジスタ６３またはＮ１レジスタ６４に格納する。

【００３３】

たとえば、ｅレジスタに１０２４ビットの演算データを格納する場合、制御回路２１は、演算回路０（４１）内のｅ０レジスタ５１に演算データのビット０～１２７を格納し、演算回路１（４２）内のｅ０レジスタ５１に演算データのビット１２８～２５５を格納し、演算回路２（４３）内のｅ０レジスタ５１に演算デ

ータのビット２５６～３８３を格納し、演算回路３（４４）内のｅ０レジスタ５１に演算データのビット３８４～５１１を格納する。

【００３４】

また、制御回路２１は、演算回路０（４１）内のｅ１レジスタ６１に演算データのビット５１２～６３９を格納し、演算回路１（４２）内のｅ１レジスタ６１に演算データのビット６４０～７６７を格納し、演算回路２（４３）内のｅ１レジスタ６１に演算データのビット７６８～８９５を格納し、演算回路３（４４）内のｅ１レジスタ６１に演算データのビット８９６～１０２３を格納する。

【００３５】

また、演算処理実行時には、１２８ビット長のレジスタ群から適宜演算データを加減算回路３５に設定することによって、各演算回路が見かけ上２５６ビット長の演算データを処理できるようになり、全体として１０２４ビット長の演算データを処理することができるようになる。また、５１２ビット長の演算データを処理する場合には、たとえばｅ０レジスタ５１、Ｙ０レジスタ５２、Ｘ０レジスタ５３、Ｎ０レジスタ５４およびＰ０レジスタ７１のみを使用することによって、５１２ビット長の演算データの処理も行なうことができる。

【００３６】

以上説明したように、本実施の形態における暗号回路によれば、レジスタ群をそれぞれ２本ずつ設け、演算回路間でキャリーアウト信号およびシフトアウト信号をループさせるようにしたので、第１の実施の形態において説明した効果に加えて、さらに演算データのビット長を容易に増やすことが可能となった。

【００３７】

（第３の実施の形態）

本発明の第３の実施の形態における暗号回路は、図７に示す第２の実施の形態における暗号回路と比較して、演算回路０～３の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００３８】

図９は、第３の実施の形態における演算回路の内部構成を説明するためのブロック図である。図８に示す第２の実施の形態における演算回路の内部構成と比較

して、演算中に繰返し使用される固定データを、演算回路による演算の前に予め計算して格納するためのＢ２Ｎ０レジスタ５５およびＢ２Ｎ１レジスタ６５が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００３９】

なお、Ｂ２Ｎ０レジスタ５５およびＢ２Ｎ１レジスタ６５を用いた演算アルゴリズムの詳細については、上述した文献を参照されたい。

【００４０】

以上説明したように、本実施の形態における暗号回路によれば、演算中に繰返し使用される固定データを予め計算してＢ２Ｎ０レジスタ５５およびＢ２Ｎ１レジスタ６５に格納しておくようにしたので、第１の実施の形態において説明した効果に加えて、特定の演算に必要となるクロック数を減らすことができ、さらに演算処理を高速に行なうことが可能になった。

【００４１】

（第４の実施の形態）

本発明の第４の実施の形態における暗号回路は、図７に示す第２の実施の形態における暗号回路と比較して、演算回路０～３の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００４２】

図１０は、第４の実施の形態における演算回路の内部構成を説明するためのブロック図である。図９に示す第３の実施の形態における演算回路の内部構成と比較して、１２８ビットのＱ０レジスタ７３およびＱ１レジスタ７４が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００４３】

演算結果を一時的に格納しておくレジスタとして、Ｐ０レジスタ７１、Ｐ１レジスタ７２以外に、１２８ビットのＱ０レジスタ７３およびＱ１レジスタ７４を設けることにより、演算結果として商と余りとをこれらのレジスタに保持することができるようになる。したがって、演算回路は、除算処理を行なうことができ

るようになる。

【００４４】

また、１０２４ビット×１０２４ビットの乗算を行なう場合、２０４８ビットの乗算結果を保持するレジスタが必要になるが、Ｐ０レジスタ７１、Ｐ１レジスタ７２、Ｑ０レジスタ７３およびＱ１レジスタ７４を用いることにより乗算結果を保持できるようになり、１０２４ビット×１０２４ビットの乗算も行なえるようになる。

【００４５】

以上説明したように、本実施の形態における暗号回路によれば、Ｐ０レジスタ７１、Ｐ１レジスタ７２以外に、１２８ビットのＱ０レジスタ７３およびＱ１レジスタ７４を設けることにより、第１の実施の形態において説明した効果に加えて、除算処理やビット長が長い演算データの乗算処理が行なえるようになり、逆元の生成処理や鍵の生成処理などの演算が行なえるようになった。

【００４６】

（第５の実施の形態）

本発明の第５の実施の形態における暗号回路は、図７に示す第２の実施の形態における暗号回路と比較して、演算回路０～３の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００４７】

図１１は、第５の実施の形態における演算回路の内部構成を説明するためのブロック図である。図１０に示す第４の実施の形態における演算回路の内部構成と比較して、１２８ビットのデータレジスタＫ０（５６）およびＫ１（６６）が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００４８】

２０４８ビットの演算データに対して演算を行なうには、合計２０４８ビットのレジスタ群を４つずつ設ければよい。この場合、演算データは、４つの演算回路０～３を４周回ることになる。また、２０４８ビットのべき乗剰余演算を行なう場合、べきｅはビット数が少なく、値が決まっており、モンゴメリ乗算剰余演

算を繰返すのに必要とされるだけである。したがって、レジスタ群をＹＹ＝｛ｅ，Ｙ｝、ＮＮ＝｛Ｂ２Ｎ，Ｎ｝、ＸＸ＝｛Ｋ，Ｘ｝、ＰＰ＝｛Ｑ，Ｐ｝などのように４本の２０４８ビットレジスタとして再定義し、２０４８ビットの演算アルゴリズムを実現するように制御回路を構成すれば、これに対応することができるようになる。

【００４９】

また、ＸＸレジスタとして使用されるＫレジスタを他のレジスタ群と同様に利用できるように制御回路を構成すれば、加減算、乗算の実行によって中国人剰余定理による合成数を法とする演算を実現できる。さらには、加減算、乗算、除算の演算結果の符号を読出す処理を追加することにより、拡張ユークリッド法による演算を実現できる。これによって、秘密鍵生成や中国人剰余定理に必要となる逆元の計算も可能となる。

【００５０】

以上説明したように、本実施の形態における暗号回路によれば、レジスタ群を再定義してビット長が長い演算データの処理も行なえるようにしたので、第１の実施の形態において説明した効果に加えて、演算に必要となるレジスタ数を削減でき、回路規模を縮小することが可能となった。

【００５１】

（第６の実施の形態）

本発明の第６の実施の形態における暗号回路は、図７に示す第２の実施の形態における暗号回路と比較して、演算回路０～３の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００５２】

図１２は、第６の実施の形態における演算回路の内部構成を説明するためのブロック図である。図１１に示す第５の実施の形態における演算回路の内部構成と比較して、右シフトイン信号と左シフトイン信号とを切替える１ビットのセレクタ８１が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００５３】

セレクタ８１は、条件選択信号によって、右シフトイン信号を選択して出力するか、左シフトイン信号を選択して出力するかを決定する。第１～第５の実施の形態においては、右シフトを実施し、左シフトを実施しない演算を行なった場合、右シフトイン信号によって入力された前段の右シフトアウトは、｛Ｑ，Ｐ｝レジスタの最上位ビットに格納されると共に、左シフト回路を経由して加減算回路３５に入力される。

【００５４】

このような回路構成の場合、右シフトイン信号が加減算回路３５に入力されるには時間がかかるため、演算回路の動作周波数を上げることが困難になる可能性がある。本実施の形態においては、右シフトを実施し、左シフトを実施しない演算の場合には、制御回路２１が条件選択信号によってセレクタ８１を切替え、加減算回路３５に直接右シフトイン信号を入力できるようにしている。

【００５５】

すなわち、第１の実施の形態においては、図５に示すようにクロックＴ２の立下りでＰレジスタ３７にデータのビット０～１２６が書込まれ、その１／２クロック後のクロックＴ３の立上りでデータのビット１２７が書込まれた。一方、本実施の形態においては、クロックＴ２の立下りでＰレジスタ３７にデータのビット０～１２６が書込まれ、その１クロック後のクロックＴ３の立下りでデータのビット１２７が書込まれる。したがって、演算回路０（４１）のＰレジスタ３７へのビット１２７の書込み時において、上位の演算回路１（４２）の右シフトアウト信号からのタイムマージンが、第１～第５の実施の形態と比較して増加するし、より高い動作周波数で暗号回路を動作させることが可能となる。

【００５６】

以上説明したように、本実施の形態における暗号回路によれば、セレクタ８１によって、右シフトイン信号と、｛Ｑ，Ｐ｝レジスタ、左シフト回路３８を経由した右シフトイン信号（左シフトイン信号）とを切替えるようにしたので、第１～第５の実施の形態において説明した効果に加えて、右シフトイン信号をＰレジスタ３７に書込む時のタイムマージンを増加させることができ、暗号回路の動作周波数を高くすることが可能となった。

【００５７】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【００５８】

【発明の効果】

請求項１に記載の暗号回路によれば、第１の演算回路の加減算回路は、第２の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を第３の演算回路へ出力するので、演算データのデータ長が長くなってもキャリーの伝播経路を短くでき、暗号回路の動作クロック周波数を高くすることが可能となった。

【図面の簡単な説明】

【図１】　本出願人が出願した出願書類に記載された暗号回路の概略構成を示すブロック図である。

【図２】　演算回路１２の概略構成を示すブロック図である。

【図３】　本発明の第１の実施の形態における暗号回路の概略構成を示すブロック図である。

【図４】　演算回路０～３（２２～２５）の内部構成を説明するためのブロック図である。

【図５】　演算回路における演算データの入力タイミングおよびＰレジスタ３７へのデータ書込みタイミングを説明するためのタイミングチャートである。

【図６】　演算回路における演算データの入力およびＰレジスタ３７へのデータ書込みが連続的に行なわれる場合のタイミングを説明するためのタイミングチャートである。

【図７】　本発明の第２の実施の形態における暗号回路の概略構成を示すブロック図である。

【図８】　本発明の第２の実施の形態における演算回路０～３（４１～４４

）の内部構成を説明するためのブロック図である。

【図９】　第３の実施の形態における演算回路の内部構成を説明するためのブロック図である。

【図１０】　第４の実施の形態における演算回路の内部構成を説明するためのブロック図である。

【図１１】　第５の実施の形態における演算回路の内部構成を説明するためのブロック図である。

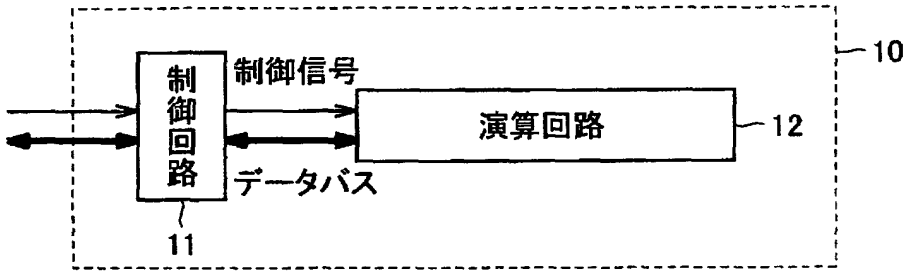
【図１２】　第６の実施の形態における演算回路の内部構成を説明するためのブロック図である。

【符号の説明】

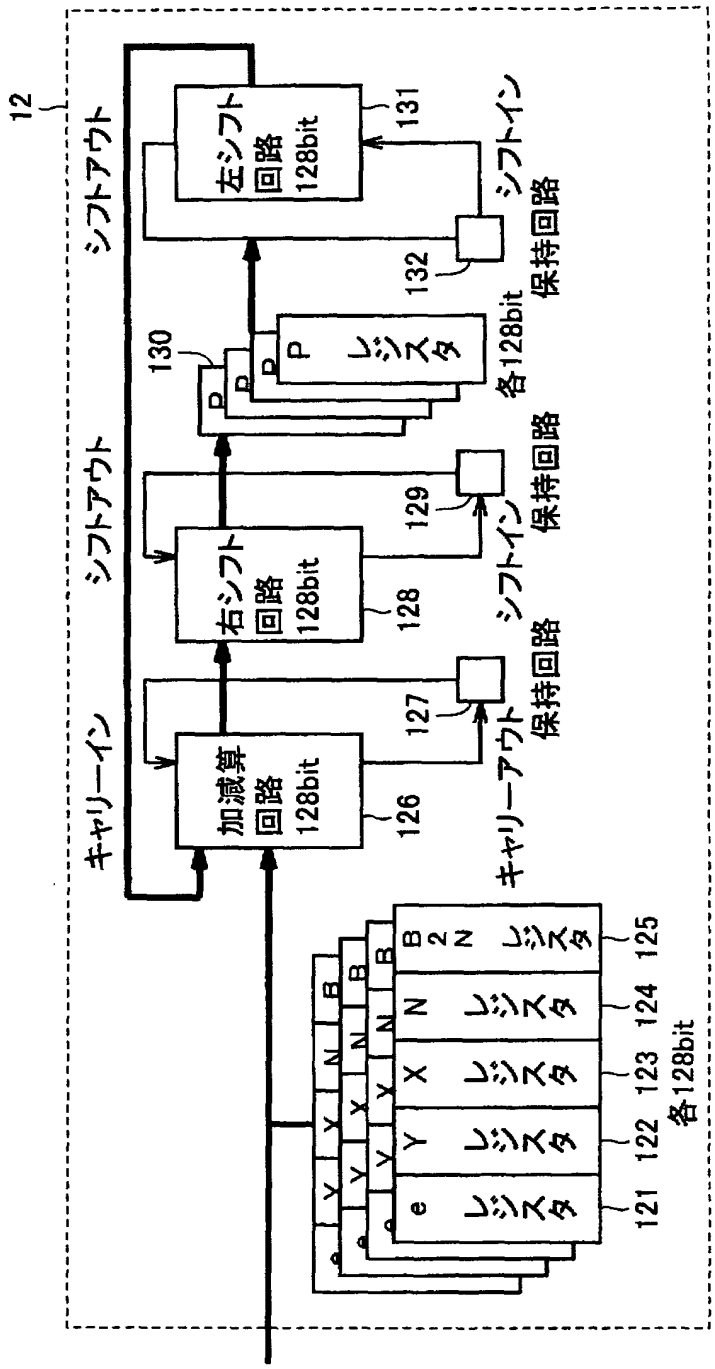
１０，２０　暗号回路、１１，２１　制御回路、１２，２２～２５，４１～４４　演算回路、３１，５１，６１，１２１　ｅレジスタ、３２，５２，６２，１２２　Ｙレジスタ、３３，５３，６３，１２３　Ｘレジスタ、３４，５４，６４，１２４　Ｎレジスタ、３５，１２６　加減算回路、３６，１２８　右シフト回路、３７，７１，７２，１３０　Ｐレジスタ、３８，１３１　左シフト回路、５５，６５，１２５　Ｂ２Ｎレジスタ、５６，６６　Ｋレジスタ、７３，７４　Ｑレジスタ、８１　セレクタ、１２７，１２９，１３２　保持回路。

【書類名】　　図面

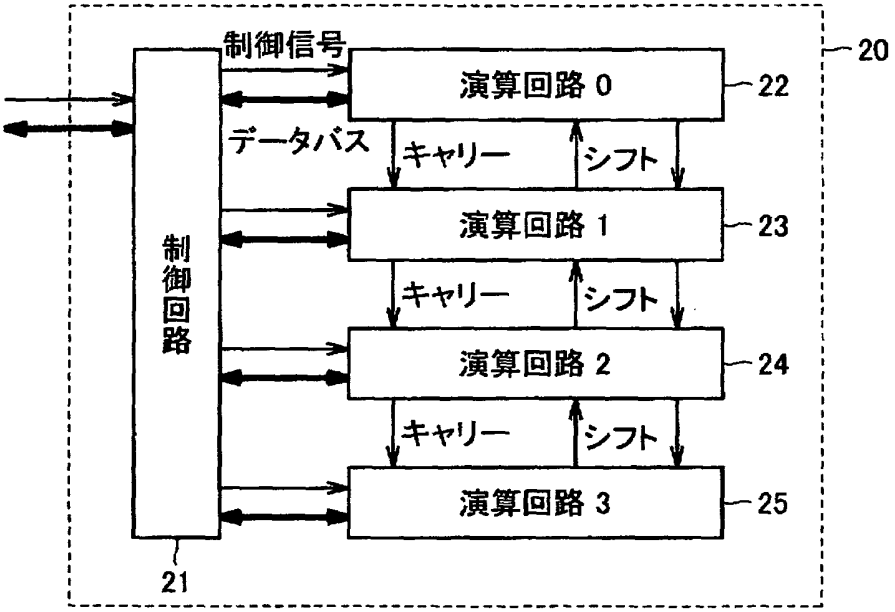
【図１】



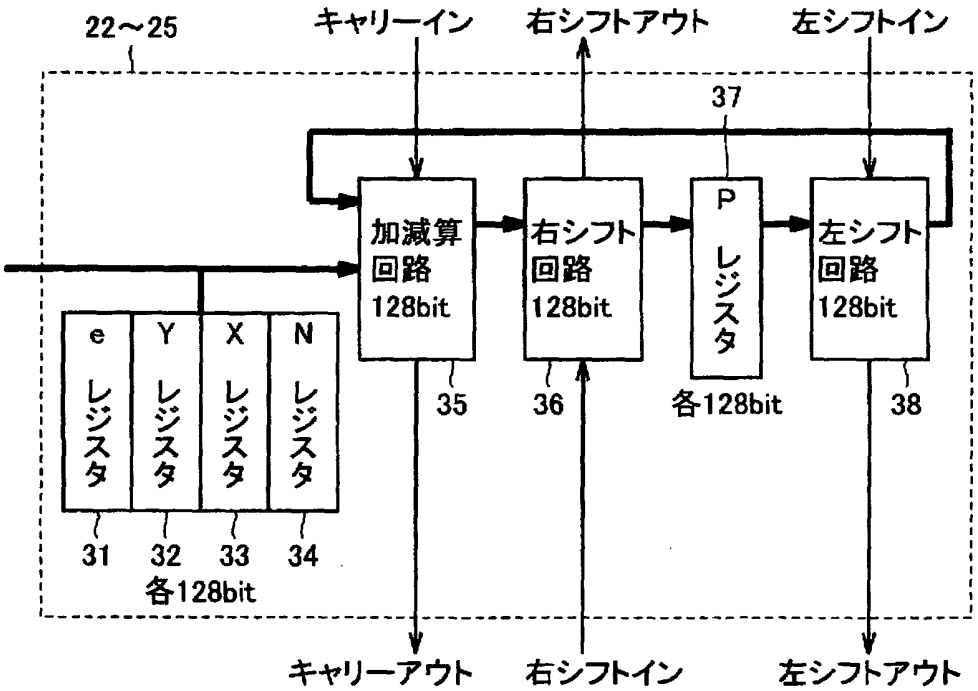
【図２】


12
キャリーイン
シフトアウト
加減算回路 128bit
126
キャリーアウト保持回路
127
右シフト回路 128bit
128
シフトイン保持回路
129
左シフト回路 128bit
131
シフトイン保持回路
132
130
P レジスタ
各128bit
e レジスタ
Y レジスタ
X レジスタ
N レジスタ
B 2N レジスタ
121 122 123 124 125
各128bit

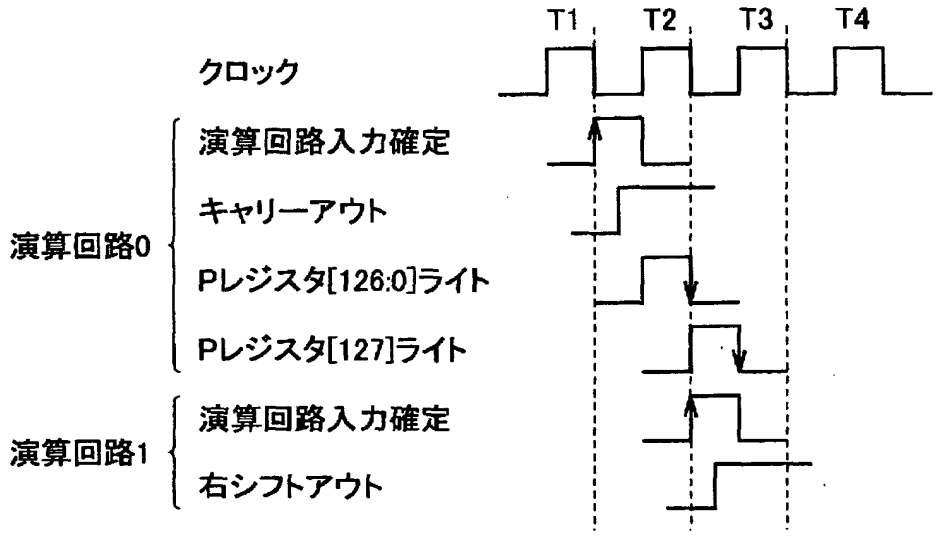
【図３】


制御信号
データバス
制御回路
演算回路 0
演算回路 1
演算回路 2
演算回路 3
キャリー
シフト
キャリー
シフト
キャリー
シフト
20
22
23
24
25
21

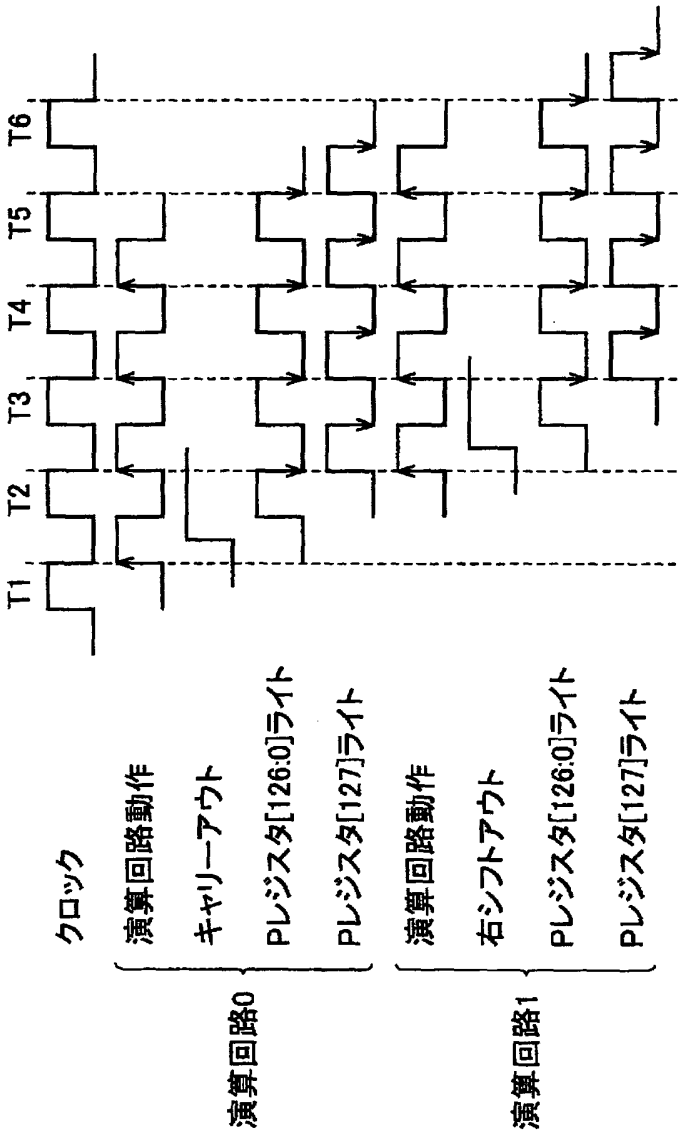
【図４】


22～25
キャリーイン
右シフトアウト
左シフトイン
37
加減算回路 128bit
右シフト回路 128bit
P レジスタ
左シフト回路 128bit
e レジスタ
Y レジスタ
X レジスタ
N レジスタ
31
32
33
34
各128bit
35
36
各128bit
38
キャリーアウト
右シフトイン
左シフトアウト

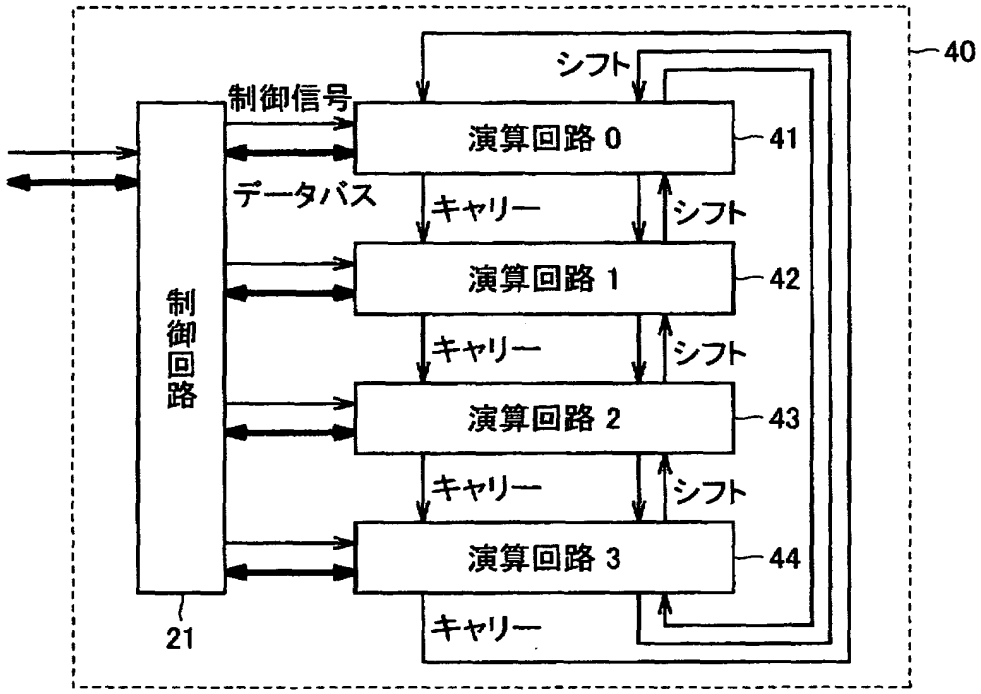
【図５】


T1
T2
T3
T4
クロック
演算回路0
演算回路入力確定
キャリーアウト
Pレジスタ[126:0]ライト
Pレジスタ[127]ライト
演算回路1
演算回路入力確定
右シフトアウト

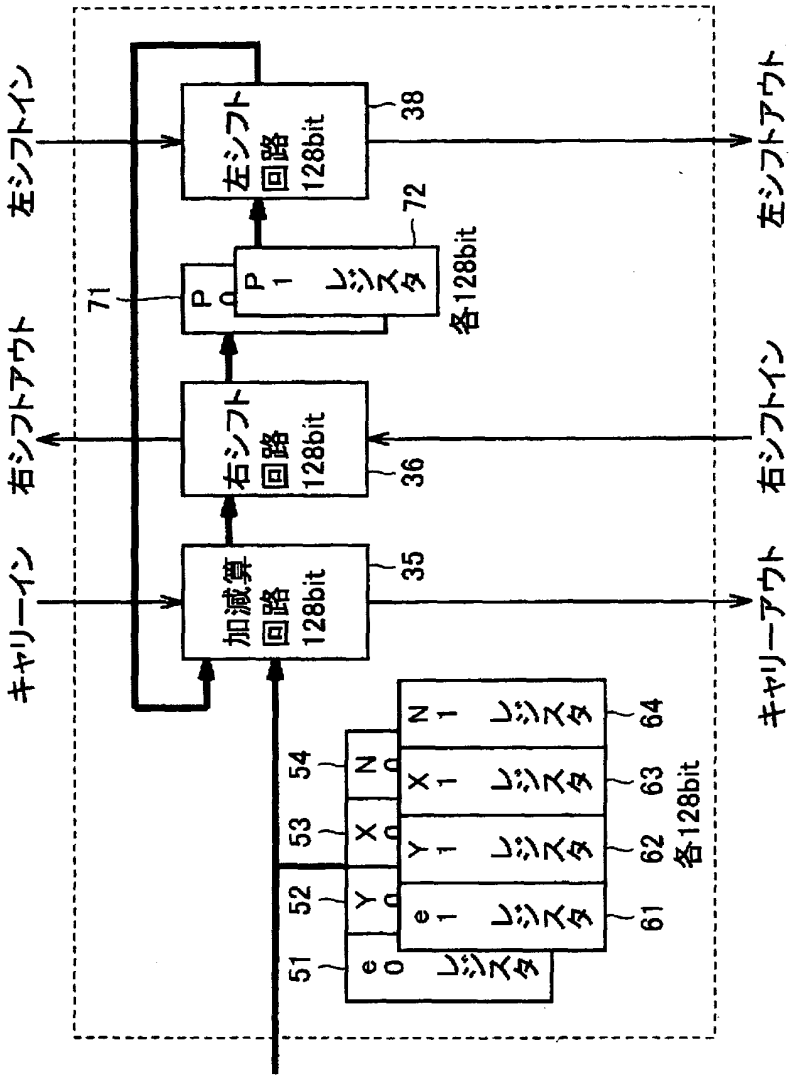
【図６】


T1
T2
T3
T4
T5
T6
クロック
演算回路動作
キャリーアウト
Pレジスタ[126:0]ライト
Pレジスタ[127]ライト
演算回路0
演算回路動作
右シフトアウト
Pレジスタ[126:0]ライト
Pレジスタ[127]ライト
演算回路1

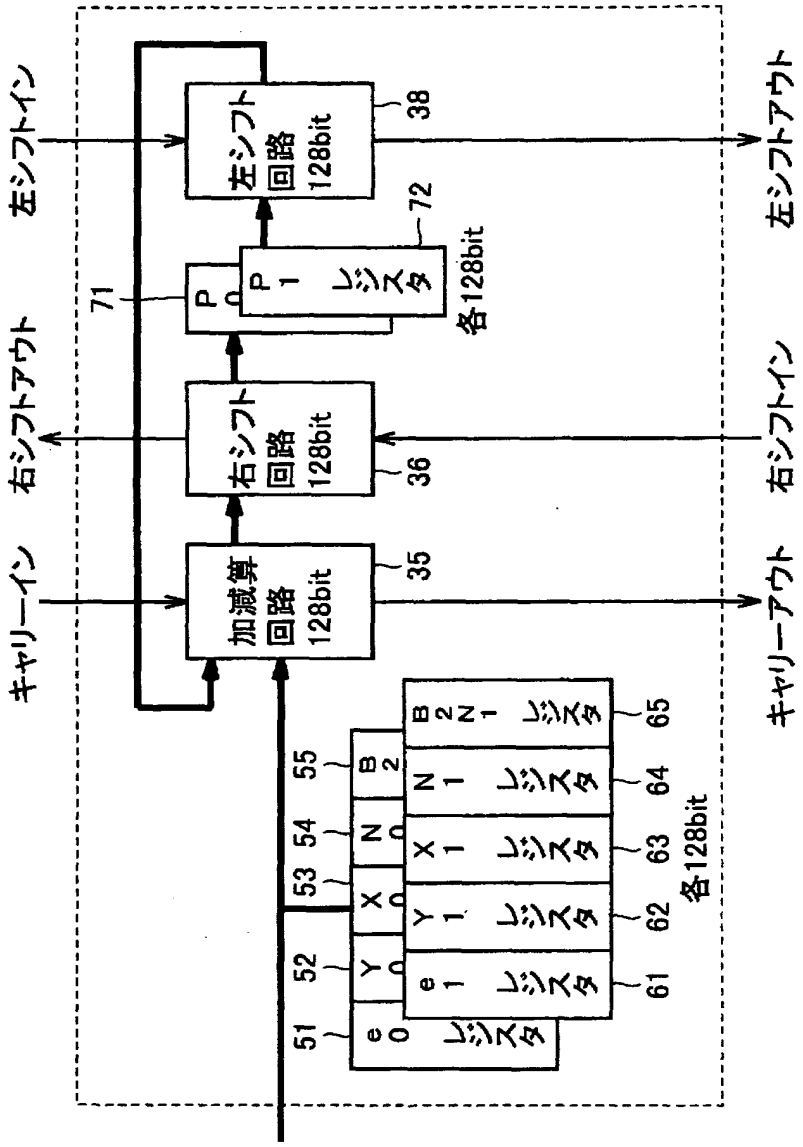
【図７】


40
シフト
制御信号
演算回路 0
41
データバス
キャリー
シフト
演算回路 1
42
制御回路
キャリー
シフト
演算回路 2
43
キャリー
シフト
演算回路 3
44
キャリー
21

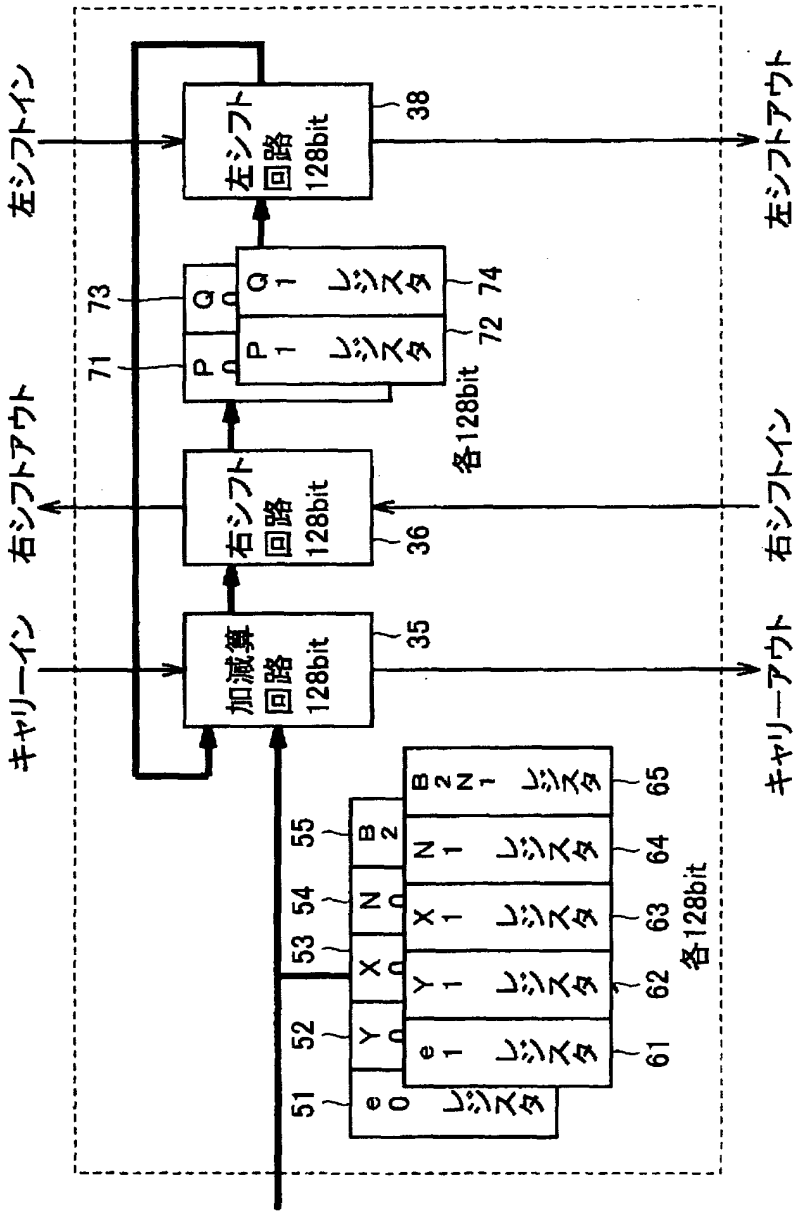
【図８】


左シフトイン
左シフトアウト
右シフトアウト
右シフトイン
キャリーイン
キャリーアウト
左シフト回路 128bit
右シフト回路 128bit
加減算回路 128bit
38
36
35
71
72
各128bit
51
52
53
54
61
62
63
64
各128bit
e 0 レジスタ
Y 0
X 0
N 0
e 1 レジスタ
Y 1 レジスタ
X 1 レジスタ
N 1 レジスタ
P 0
P 1 レジスタ

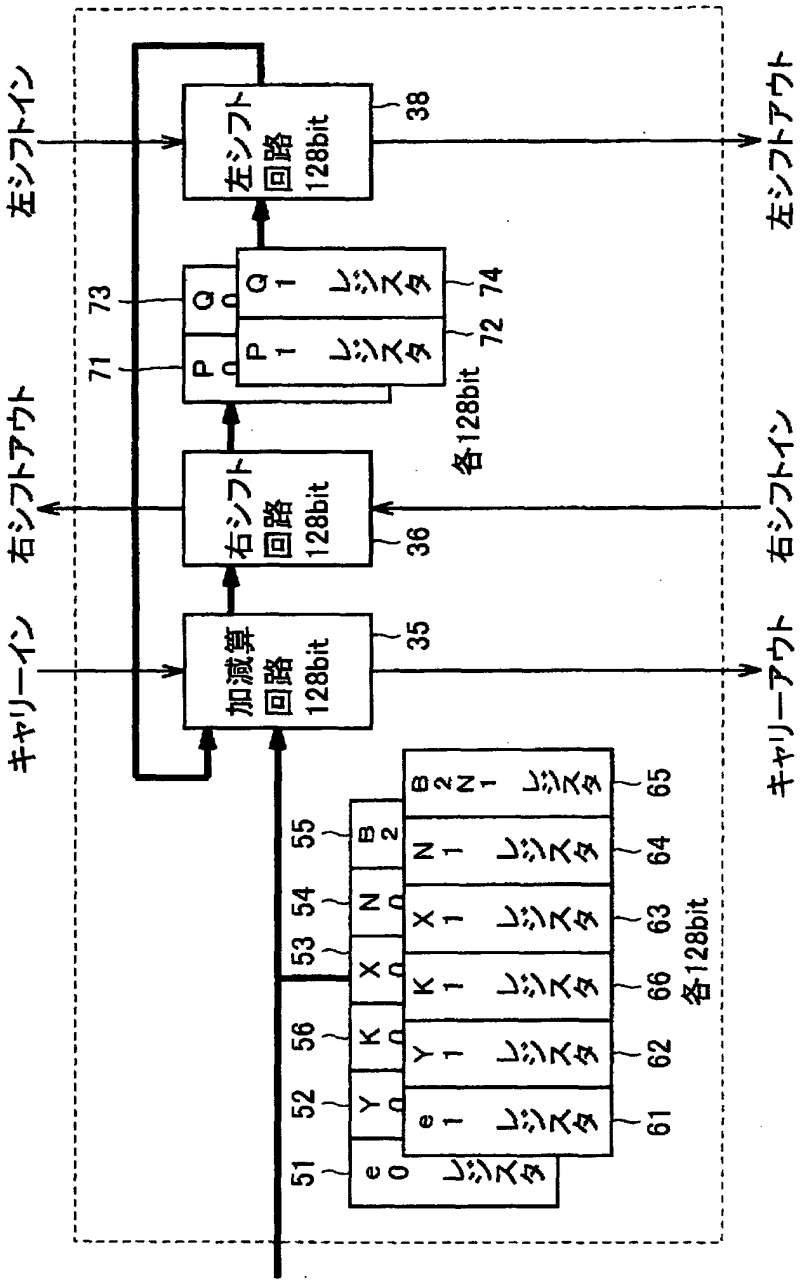
【図９】


左シフトイン
左シフトアウト
右シフトアウト
右シフトイン
キャリーイン
キャリーアウト
左シフト回路 128bit
右シフト回路 128bit
加減算回路 128bit
38
36
35
71
72
各128bit
51
52
53
54
55
65
64
63
62
61
各128bit

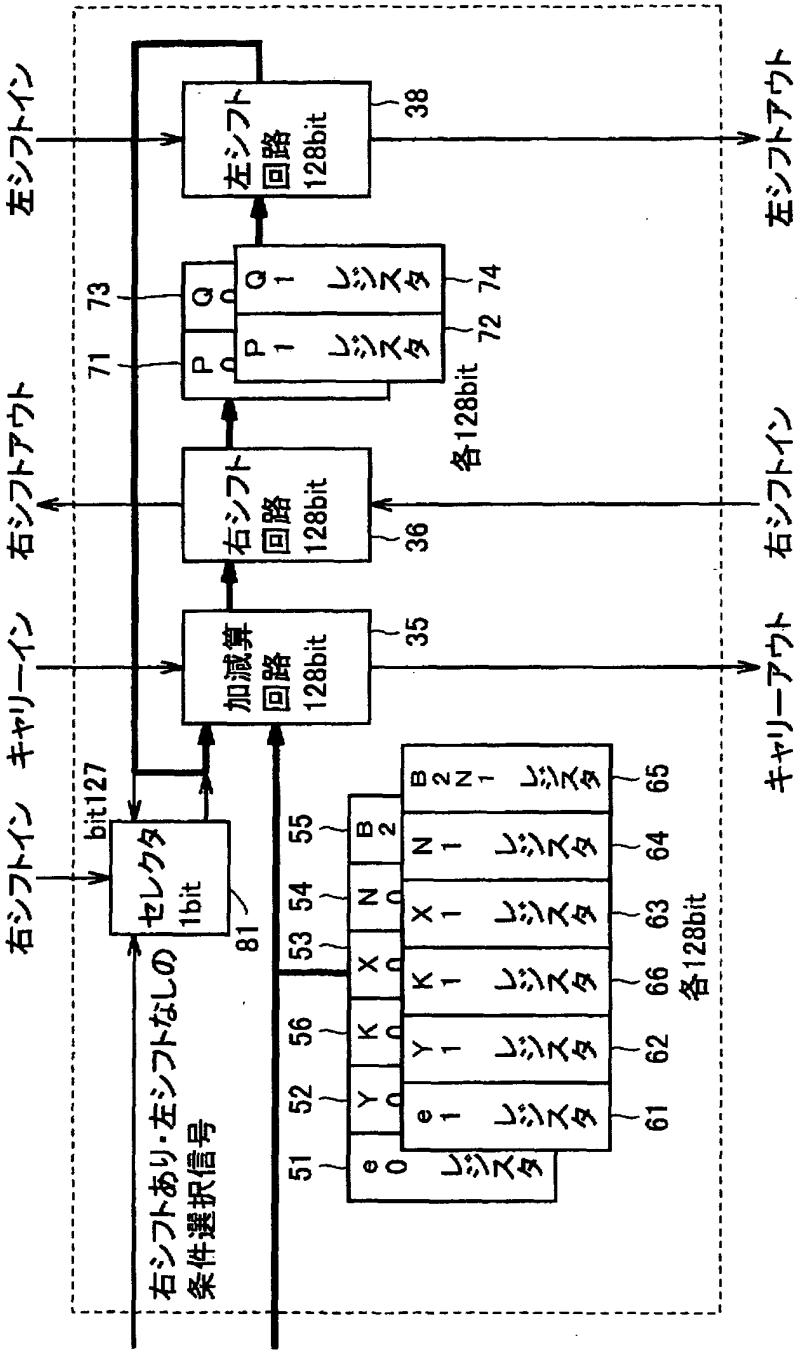
【図１０】


左シフトイン
左シフトアウト
左シフト回路 128bit
38
右シフトアウト
右シフトイン
右シフト回路 128bit
36
キャリーイン
キャリーアウト
加減算回路 128bit
35
P 0
P 1 レジスタ
Q 0
Q 1 レジスタ
71
73
72
74
各128bit
e 0 レジスタ
e 1 レジスタ
Y 0
Y 1 レジスタ
X 0
X 1 レジスタ
N 0
N 1 レジスタ
B 2
B 2N-1 レジスタ
51
52
53
54
55
61
62
63
64
65
各128bit

【図１１】


左シフトイン
左シフトアウト
左シフト回路 128bit
38
右シフトアウト
右シフトイン
右シフト回路 128bit
36
キャリーイン
キャリーアウト
加減算回路 128bit
35
71
73
P 0
Q 0
P 1 レジスタ
Q 1 レジスタ
72
74
各128bit
51
52
56
53
54
55
e 0 レジスタ
Y 0
K 0
X 0
N 0
B 2
e 1 レジスタ
Y 1 レジスタ
K 1 レジスタ
X 1 レジスタ
N 1 レジスタ
B 2N-1 レジスタ
61
62
66
63
64
65
各128bit

【図１２】


左シフトイン
左シフトアウト
左シフト回路 128bit
38
右シフトアウト
右シフトイン
右シフト回路 128bit
36
キャリーイン
キャリーアウト
加減算回路 128bit
35
右シフトイン
bit127
セレクタ 1bit
81
右シフトあり・左シフトなしの条件選択信号
71
73
P 0
Q 0
P 1 レジスタ
Q 1 レジスタ
72
74
各128bit
51
52
56
53
54
55
e 0 レジスタ
Y 0
K 0
X 0
N 0
B 2
e 1 レジスタ
Y 1 レジスタ
K 1 レジスタ
X 1 レジスタ
N 1 レジスタ
B 2N-1 レジスタ
61
62
66
63
64
65
各128bit

【書類名】　　要約書

【要約】

【課題】　暗号回路の動作クロック周波数を高くでき、演算速度の高速化を図ることが可能な暗号回路を提供すること。

【解決手段】　加減算回路３５は、他の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を他の演算回路へ出力する。また、右シフト回路３６は、他の演算回路からのシフトイン信号を用いて右シフトを実行し、右シフトによって発生するシフトアウト信号を他の演算回路へ出力する。したがって、演算データのデータ長が長くなってもキャリーの伝播経路を短くでき、暗号回路の動作クロック周波数を高くすることが可能となる。

【選択図】　　図４

出　願　人　履　歴　情　報

識別番号　〔０００００６０１３〕

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社